International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 2, Apr 2014, 245-252


TRANS STELLAR
• Journal Publications • Research Consultancy

# CRYPTOGRAPHY COMBINED WITH STEGANOGRAPHY FOR ENCRYPTION: STUDY AND COMPARISON

**MANALI TAWDE, HEENA PARULEKAR & SWAPNIL SHINDE**

Department of Information Technology, RAIT, Nerul, Mumbai, Maharashtra, India

## ABSTRACT

Internet is a big means for transferring lot of data in the form of images, text, and all multimedia. Data security is a major concern in terms of its availability, confidentiality and authentication goals. Communication channel security also plays an important role, but channel can be compromised so there is need of data security. Images serve a means for transferring lot of data secretly, many techniques have been proposed which use images to carry lot of secret data for this encryption is best method. Cryptographic algorithms include symmetric and asymmetric techniques and hash function for encryption purpose. The paper discusses techniques that use RSA, DES, AES, MAES algorithms applied on images along with orthogonal transforms for Image. The comparison parameters considered here are the cryptographic techniques, algorithm applied, type of algorithm and performance parameter.

**KEYWORDS:** AES, Correlation Coefficient, DES, DWT, Encryption, Hash Function, PSNR

## INTRODUCTION

Encryption is a technique which is used to maintain the security of the image. Applications of image and video conferencing are internet communication, multimedia systems, medical imaging, Tele-medicine and military communication [1]. As the technology has become more advanced multimedia data is being used more widely in applications like video-on-demand, video conferencing, and broadcasting. Most of the encryption algorithms have been widely used i.e. AES, RSA and IDEA which is used on text or binary data. Digital image encryption is one of the secure methods for protecting the images against illegal copying while transferring over an insecure channel.

In cryptography the original message is transformed into cipher text message so that it cannot be understood by the intruders but there is a possibility that the intruder might be actively curious to know what information is being transferred over the channel [1]. On the contrary, a sensible method of covering the original message into another media would provide more data integrity, as the observer will not have any idea that the message being transferred has any hidden information. This method is called as steganography. The word steganography has been derived from a Greek word steganos means cover and grafia means writing [2][4].

The stego image should not differ from the original cover image. The information is encrypted by a combination of cryptography and steganography to provide a high level of integrity. Cryptography hides or encrypts the information and steganography ensures that the data is hidden. Thus a high level of data integrity is maintained. Steganography includes watermarking concept where a signal or watermark is added to the original image to hide it [3].

## TYPES OF CRYPTOSYSTEM

The types of crypto system are as follows:

- Symmetric(private) key cryptography
- Asymmetric(public)key cryptography

### Hash Functions

Symmetric Key system involves use of single key for encryption and decryption. It has mainly two categories stream cipher and block cipher [1]. Some of the most well known block cipher include DES, AES and stream cipher include RC4.

DES [5] is block cipher used for encryption of 64 bit block using a 56 bit key. It includes a key generation block and round function which contains many operations like permutation, expansion, substitution and Xoring. There are 16 rounds in DES where a new key is generated for each round. The DES was advanced to double DES and 3DES [1][5] by increasing the size of the key for improving the security. AES is block cipher with variable key size of 128,192 or 256 applied on same size blocks using rounds varying from 10 to 14. In terms of Asymmetric key system, RSA [5] is most widely used algorithm for encryption purpose along with Diffie Hellman key exchange and Digital signatures.

RSA can be summarized as follows:

- Choose two prime numbers, 'p' and 'q'. From these numbers you can calculate the modulus, n = pxq.
- Select a third number 'e' that is relatively prime to the product (p-l )(q-l ). The number 'e' is the public exponent.
- Calculate an integer 'd' from the quotient (ed-l ) / [(p-l )(q- l )]. The number 'd' is the private exponent.

The public key pair is (n,e) and private key pair is (n,d). Hash Functions are also called message digest and are used to maintain the integrity of the message while it is transferred via a medium. Hash functions [5] is one of the way which generates a hash value that is unique and is irreversible. Mostly used hash functions are SHA, MD5 and Tiger hash respectively.

## STEGANOGRAPHY TECHNIQUES

- **Substitution in Spatial Domain [6]:** This include Data hiding by least significant beat, Pixel value difference and gray level modification.
- **Transform Domain Technique:** This uses transform coefficients to hide the data which makes it more robust from attacks related to compression etc. The transforms used in this technique are DCT and DWT [7].
    - **DCT:** It uses JPEG compression to convert 8x8 pixel block to 64 DCT, applied in frequency domain.
    - **DWT:** This technique uses haar transform where the secret data is stored in the least coefficient of 4x4 transform blocks.
- **Spread Spectrum Technique:** Message is spread over frequency band rather than keeping it in limited bandwidth.

- **Statistical Technique:** It applies some mathematical calculations over the image pixel values.
- **Distortion Technique**: Information is stored by signal distortion by adding some cover which results in minor changes. These changes are then decoded by the decoder.

## PROPOSED TECHNIQUES: STUDY

The first foremost and most commonly cryptographic algorithm known is the RSA algorithm. The study of this paper starts with a technique proposed **Nadiya P V & Mohammed Imran [7]** which is steganography in DWT domain using double stegging with RSA encryption.

The central idea of this model is cryptography and steganography which is achieved in two stages.

**Stage 1: Encryption Using RSA algorithm**

RSA is the the most widely used public key cryptography algorithm. This algorithm has been named after its founders Rivest, Shamir and Adleman. This algorithm produces cipher text along with public and private keys. The cipher text is then converted into 8-bit binary code for further procesing in the second stage.

**Stage 2: Embedding Using Double Stegging**

This stage carries out the embedding of the binary data on the cover image. It utilizes the 2D-DWT transform coefficients using haar's wavelet for embedding process. This transform provides one approximation coefficient and three detail coefficients. The secret data is embedded on any of the detail coefficients .The approximation coefficient is not used for secret data embedding as it carries the information content of the whole cover image.

**Step 1:** Steganography is applied to cover image in order to embed the encrypted data into one of the detail coefficients which results in stego-image.

**Step 2:** Steganography is again applied to embed that detail coefficient to another area of detail coefficient of that image. The image with secret data is then ready for transmission. The extraction process also requires 2 steps for decoding

**Step 1:** The decoding process is done to extract the first detailed coefficients from the second detail coeficient.

**Step 2:** The second decoding involves extraction of secret data from first detail coefficient. This process includes simple modulo operations of stego-image coefficients. The final stage at the receiver side include the decryption process of the cipher text by private key using RSA algorithm.

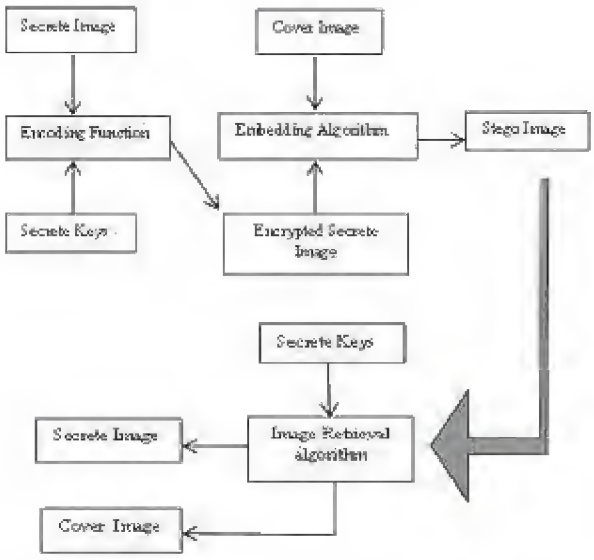


**Figure 1: Block Diagram of Steganography Using DES**

The model proposed by **Manoj Kumar Ramiya et.al** [8] is based on DES function which consists diffusion, S-box mapping and secret key. Refer Figure 1.

**Encryption Process**

- The secret image and secret key are applied as inputs to the encoding function for encrypting the secret image.
- The encrypted secret image and the image that is to be used to cover the secret image are provided to the embedding algorithm. The embedding algorithm embeds the cover image over the secret image and the new produced image is called as stego image.

**Decryption Process**

- The image retrieval algorithm along with the secret key decrypts the image i.e. it retrieves the secret image from the stego image by separating the secret image from the cover image.

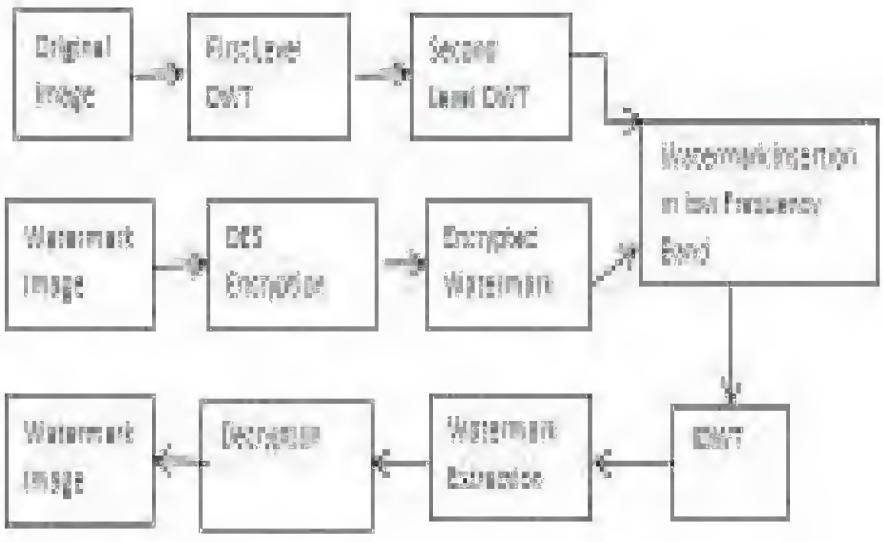

**Figure 2: Block Diagram of Watermarking Algorithm with Encryption Using DES**

**Nirupama Tiwari** et.al.[9] proposed digital watermarking technique using DWT domain and DES for encryption of the water marked image that is used for watermarking the original image. Original image is selected, DWT transform is applied up to second level of decomposition to obtain four bands. DWT compresses the image and the low band of decomposition contains maximum information related to the original image. A watermarked image is chosen and symmetric algorithm of DES is applied to obtain an encrypted watermark image. The watermark image is divided in blocks of size 8x8, a key of 64 bits is generated and then DES is applied on the image with the above key. Thus an encrypted watermark is generated which is then embedded to the Lower band obtained of the original image. This gives a completely encrypted image using a watermark and DES.

The watermark extraction process is of two types: blind and non-blind. This system uses a non-blind where we select an original image and from that we recover the watermark image. Refer Figure 2.

Modified AES for Image Encryption was proposed by **Seyed Hossein Kamali** et.al [10]. A more efficient and secure algorithm was developed to overcome the disadvantages of AES algorithm by adjusting the shift row transformation. Shift row transformation:

The first step is to identify the value in the 1st row and 1st column whether it is even or odd i.e. state[0][0]

If the value is odd, then the 1st and the 3rd row remain unchanged and the bytes from the 2nd row are shifted 1 to the left and the 4th row is shifted 3 to the left.

If the value is even, then the 1st and the 4th row remain unchanged and the bytes from the 2nd row are shifted 3 to the right and the 3rd row is shifted 2 to the right.

A Novel Image encryption method using hash function proposed by **Seyed Mohammad Seyedzade** et.al [11][12] uses SHA-2 for encryption. The system applies substitution-diffusion architecture for image based cryptosystem as shown in Figure 3. Four stages are involved which are combination of substitution and diffusion process for Image encryption. The architecture of substitution-diffusion type SHA-2(512) based image cryptosystem is shown in Figure 2. There are four stages in this type of SHA-2 based image cryptosystem. The first two stages have two processes of substitution and diffusion and last two stages have only diffusion process. Single pixel out of four are replaced by using S-box method, diffusion involves making slight change sequentially in pixel value that will affect the entire image. Substitution is carried out to change the relation between neighboring pixels. Diffusion is then carried out, this way substitution diffusion keeps on repeating till a satisfactory level of security is achieved. Larger image is divided into blocks of four sub images (namely *Se.*1, *Se.*2, *Se.*3 and *Se.*4 images). In order to better understand the structure, First Equivalent description of the cryptosystem will be presented and then the cores of each stage is introduced.

- Equivalent description of the cryptosystem*:* Equivalent description is as follows:
  - Substitute the sub-image Se.x according to S-box of AES (*Sbox*(*Se.x*)): Substitute a quarter of the image pixels according to the S-box of AES.
  - The mean of columns of each row in *Se.x* sub-image (*MCR*(*Se.x*)): For *Se.x* sub-image, XOR all the gray level values of row *i*, where $x = 1, 2, 3, 4$ and $i = 1, 2, \ldots, 128$. As a result, a matrix of size $128 \times 1$ is obtained. For a mask, concatenate the matrix horizontally.

- The mean of rows of each column in *Se.x* sub-image (*MRC*(*Se.x*)): For *Se.x* sub-image, XOR all the gray level values of column *i*, where $x = 1, 2, 3, 4$ and $i = 1, 2, \cdots, 128$. As a result, a matrix of size $1 \times 128$ is obtained. For a $128 \times 128$ mask, concatenate the matrix vertically 128 times.
- Sub-images Hashing (Hash(*Se.x*, *Se.y*)): Sub-images *Se.x* and *Se.y* forms a matrix of size $128 \times 256$ called *M*. Each row of *M* is divided into four sub arrays with size of 124 bytes. In addition, four 8-bit keys will be appended to each of these sub arrays.

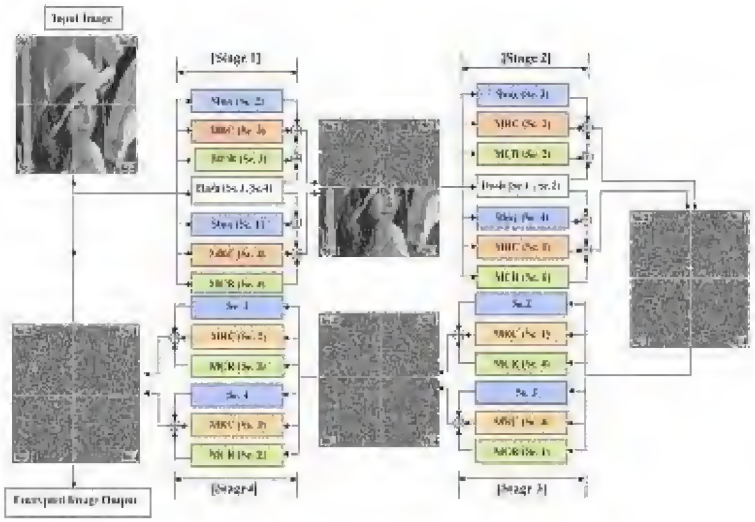

**Figure 3: The Overall Architecture of Substitution-Diffusion Type SHA-2(512) Based Image Cryptosystem**

## COMPARISON

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | Technique proposed | DWT+RSA [7] | DES+Steganography[8] | DWT+DES [9] | MAES[10] | Hash Function[11] |
| 2 | Type of cryptography | Asymmetric | Symmetric | Symmetric | Symmetric | One way Hash |
| 3 | Approach | DWT | LSB | DWT | Shift Row | Substitution Diffusion |
| 4 | Algorithm | RSA | DES | DES | MAES | SHA-2 |
| 5 | Performance Parameters | PSNR | PSNR | Correlation Coefficient | Correlation coefficient, Entropy Value | Correlation coefficient, Histogram |
| 6 | Advantages | Lower risk of Discloser, Best PSNR | Flexibility, Robustness, image quality improvement | Efficient and easy | More efficient, High Security | Ensures input sensitivity, High Security |

## CONCLUSIONS

With the development of digital technology and internet it becomes a prime concern to protect the digital data like images, video and multimedia from various attacks by means of different techniques. The multimedia can be easily attacked and information can be retrieved easily. Many systems are proposed to maintain the security of data by applying cryptographic algorithms, these algorithms can also be applied on the images for encryption purpose. Steganography is another means for protecting images from attacks and hiding lot of valuable information in the images. We have studied

different systems which are combination of cryptography and steganography for maintaining security and robustness along with integrity of the data. Overall study of different proposed system for image encryption show that cryptographic algorithms like RSA, DES, Hash function in combination with steganography domains like DWT , LSB provide very high level of security, flexibility which is measured by means of various statistical analysis methods like PSNR , Correlation coefficient , entropy value.

## REFERENCES


1. Gary C. Kessler , 'An overview Cryptography' June 2010.
2. Shashikala Channalli, Ajay Jadhav, 'Steganography an art of hiding data', IJCSE, Vol.1 (3), 2009, 137-141.
3. Jonathan Cummins, Patrick Duskin, 'Steganography and Digital watermarking', University of Birmingham, 2004.
4. Prabhjot Kaur and Reena, 'Watermarking embedding in Spatial domain', IJETTE-ISSN: 2320-9569, Vol. 5, July 2013.
5. Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, 'New Comparative study between DES, 3DES and AES within Nine factors' , Journal of Computing, Vol. 2, Issue 3, 2010.
6. Riah Ukur Ginting Rocky Yefrenes Dillak , 'Digital Color image Encryption using RC4 Stream cipher and Chaotic Logistic Map' IEEE, 2013.
7. Nadiya P V, B Mohammad Imran, 'Image Steganography in DWT domain using Double-stegging with RSA Encryption' , ICSIPR , IEEE, 2013.
8. Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena, 'Security Improvisation in Image Steganography using DES ', IEEE IACC, 2013.
9. Nirupama Tiwari, Manoj Kumar Ramaiya, Monika Sharma, 'Digital Watermarking using DWT and DES', IEEE IACC, 2013.
10. Seyed Hossein Kamali, Maysam Hedayati, Reza Shakerian, Mohsen Rahmani , 'A new modified version of Modified Advanced Encryption Standard Based algorithm for Image Encryption', IEEE ICEIE, 2010.
11. Seyed Mohammed Seyedzade, Reza Ebrahimi Atani, Sattar Mirzakuchaki, 'A Novel Image Encryption Algortihm based on Hash Function', IEEE, 2010.
12. Komal D Patel, Sonal Belani, 'Image Encryption using Different techniques: A Review', IJETAE, Vol.1, Issue 1, 2011.